

Exhibit A



JOSHUA M. FEASEL
ATTORNEY AT LAW

P.O. BOX 6842
DETROIT, MI 48206
734.726.0016
JOSH@FEASELPLLC.COM

August 3, 2020

Ian C. Downie Theodore A. Fons Eugene A. Shimshock, II
ian@patronpoint.com ted@patronpoint.com gene@patronpoint.com

Patron Point, Inc. Ohio Registered Agent Service, LLC 6545 Market Ave. North, #100 North Canton, OH 44721	Third Chapter Partners, LLC (d/b/a Patron Point) 6418 Newgrange Drive Dublin, OH 43016
--	---

**Re: Demand to cease and desist efforts to breach the
security of OrangeBoy, Inc.**

Dear Messrs. Downie, Fons, and Shimshock:

I write on behalf of my client, OrangeBoy, Inc., regarding a serious matter. In short: OrangeBoy has uncovered evidence that someone associated with Patron Point has been trying to hack into OrangeBoy's servers.

OrangeBoy has earned its clients' trust by taking security very seriously. It spends significant time and energy ensuring the continued privacy of both its own and its clients' confidential data, and it maintains strict procedures and security protocols to help it do so. In recent months, OrangeBoy's security team observed a number of attempts to gain unauthorized access to the company's servers, primarily through efforts to guess and reset the user passwords for OrangeBoy users. Recently, however, these efforts intensified. In just the last week, OrangeBoy has observed not only further attempts to guess and reset user passwords for OrangeBoy users, but also (1) attempts to guess and reset passwords for users associated with OrangeBoy's *clients*; (2) the use of a fake name and institutional affiliation to seek technical information about OrangeBoy's services; and (3) an apparent attempt to overwhelm OrangeBoy's servers or to obscure these other intrusion efforts through an "email subscription bomb."

OrangeBoy's investigation into these escalating attacks strongly suggests that someone associated with Patron Point is responsible for them.

We do not make these serious allegations lightly. Efforts to hack into a competitor's computer system are illegal under federal and state law, and such conduct could subject the hacker to significant criminal and civil liability. Moreover, as you can surely imagine, a successful intrusion into OrangeBoy's servers would significantly harm our industry as a whole by weakening trust in the security and confidentiality of library cardholder data.

For those reasons, we cannot imagine that this conduct would take place with the knowledge and approval of Patron Point's senior management. We therefore write in hopes that once you are made aware of the situation, you will take appropriate steps to remedy it and make sure that it will not recur. In particular, we ask that you:

- (1) Immediately cease and desist the conduct described above, as well as any other attempts to obtain unauthorized access to OrangeBoy's servers, to overload or otherwise damage OrangeBoy's computer systems, or to obtain information from OrangeBoy by false pretenses;
- (2) Investigate the circumstances under which those efforts were undertaken;
- (3) Identify and immediately terminate the employment of all persons responsible for such actions; and
- (4) Implement policies and practices to ensure that no one affiliated with Patron Point will engage in similar behavior in the future.

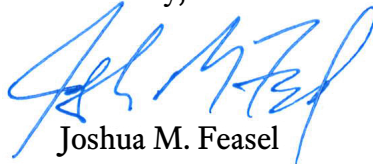
We would be glad to work with your security team to help them track down the source of this misconduct. Please just let us know how we can help.

Given the seriousness of this matter, we ask that you act promptly to address our requests. Please confirm as soon as possible that you are investigating the matter, and in any event let us know by the end of the day on Monday, August 10, 2020, what steps you have taken to remedy the situation.

Although we sincerely hope to resolve this matter amicably, OrangeBoy reserves its right to take further action to remedy this conduct, including legal action if necessary. Accordingly, we ask that you take steps to preserve all information in your possession, custody, or control regarding this matter. This includes emails, text messages, server and activity logs, social-media accounts, and any other information that falls within the scope of Rule 34 of the Federal Rules of Civil Procedure. The failure to preserve any relevant information—even if that information is destroyed through automatic processes or standard document-destruction policies—may be grounds for sanction by a court of law.

Thank you for looking into this matter. We hope to hear from you soon.

Sincerely,



Joshua M. Feasel

cc: Sandra Swanson
M. Clark Swanson II
Christopher Kelbley